整数論のソフトウェアとデータベースについての提案(代数的整数論)

AUTHOR(S):

中村, 憲

CITATION:

中村, 憲. 整数論のソフトウェアとデータベースについての提案(代数的整数論). 数理解析研究所講究録 1991, 759: 118-124

ISSUE DATE:

1991-06

URL:

http://hdl.handle.net/2433/82193

数理解析研究所講究録
第759巻 1991年 118-124

118

整数論のソフトウェアとデータベースについての提案

東京都立大学 理学部　　中村 憲 (Ken Nakamula)

1　趣旨

目的 既知の公式やアルゴリズムなどを利用して, 実際にコンピュータで整数論の不変量を計算するとき, その手順や計算効率, 実効性などが問題となり, あまり手軽には実行出来ない. そこでソフトウェアを協力して開発し, データベースを共有する事により, その困難を少しでも解消する事に役立てたい. 更に, その中から整数論の新たな理論的進展が生まれる事と, 又逆に計算機科学に対する整数論の要請が体系的に解明される事とを期待する.

動機 この様な事を始めた契機には実用と理論と両面ある.

実用面 整数論の各分野における実例計算や数値計算は, 不変量などを具体的に計算して求める一般的方法が知られて居ながら, コンピュータの利用が不可欠な為に手軽に誰でもが出来ない場合も多かった. しかし近年のコンピュータの能力の向上と利用可能性の増大によって, これら複雑で大量の計算を要する分野にも新しい光が当てられて来て居る.

その中で, 初歩的な数値実験は既に数多くあり, 幾つかの研究成果も個別に現れて居るが, それらを交流し合う場が少ない為, 未だ個人のレベルに留まって居る. 例えば百桁を越える基本単数の計算結果が印刷物として与えられても, せいぜい感心して眺めるだけで, それを次の計算の為のデータとして簡単には使えない. 計算結果を共有出来るデータベースが是非欲しい. あるいはイデアル類群の計算方法の新しい工夫がされても, そのプログラムを手に入れるのすら安易ではなく, それが他の計算にも生かされる程には中々定着しない. ソフトウェアを共有の知恵として利用出来るようにしたい. このデータベースとソフトウェアの共有は現在では不可能ではない. 実際に後述する様な数論専用のソフトウェアが開発されて来て居る.

理論面 この様な状況で今迄とは違った理論的問題も提起されて居る. 即ち計算数論 (あるいは計算整数論) と呼ばれる分野である. これは AMS の Mathematics Subject Classification に 1985 年に新たに加えられた **11Yxx Computational Number Theory** に当たる分野で, その中心的な研究テーマも未確定であろう. 特に数式処理と整数論の関係を重視する事が — 計算数論にとっても計算機科学にとっても — 必要と思うが, これに限らず新たに整数論に提起されて居る課題を討議し合い整理したい. その事は数論専用のデータベースやソフトウェアの共有なしには考えられない. 事実, 近年開催されている計算数論の国際的シンポジウムは数論専用のソフトウェアの開発の幾つかと密接に関連している.

整理の要領 現在迄の, この分野の利用可能なソフトウェアやデータベースを整理して纏める作業を次の要領で推進する.

- ゼロから出発するのではなく, まず既にある物を収集する. 収集するデータの正しさについては保証された物である必要はない. 出来るだけ, そのデータを計算したプログラム — ある程度バグがある物でも良いから — を一緒に収集する事でソフトウェアの共有を計る.
- データやプログラムの収集や配布は出来るだけ迅速にする. また, その改良も公開, 交流して共有の知識とする. その意味で, データについてはOSや機種に依存しないで誰でも読んで利用出来る形式での交流を大切にし, プログラムについては便利さよりも計算方法が誰でも読めて修正出来る様にソースプログラムの交流を大切にする. 具体的には次の様にする:
  - データは通常の可読コードで書かれて居る方が望ましい. 例えばアスキーコードで書かれた数表で, 容易に — 通常のコンヴァータでコード変換したりして — 他のプログラム等から利用出来る方が良い. そうでなければデータ形式が正確に定義された説明文の付属する物とする. もちろん何の計算結果か明示されて居る必要がある.
  - プログラムは少くともUNIX, 又はMS-DOS, 又はMAC-OS等の標準的なOS上では動く物が良いが, OSや機種に依存しない方が望ましい. 例えばCで書かれたプログラムでUNIX上で動く物で, それをMS-DOSに持っていってもメモリーの制限等を除けばそのま

ま動く物が望ましい．またそれらはC, PASCAL, MACSYMA, MATHEMATICA, COMMON LISP, FORTRAN, BASICあるいはUBASIC等の高級言語で書かれた，通常の可読コードのソースプログラムで，出来るだけ入力，出力が何であるか明示された物が望ましい．さらに標準的なOS上では動かなくても高級言語で書かれて居て，OSや機種依存の部分が分離されて居れば収集の対象とする．機械語等で書かれた物は，さらにアルゴリズムとデータ形式の詳しい説明を必要とする．

配布の際にはクレジットで提供者，作成者，修正者等を明記する．また配布された物は自由に変更したり再配布して良いが，その際に必ず変更者，変更個所，変更年月日を明記し，それを連絡センタを通じて広範に知らせる．データやプログラムの読み取りを困難にする暗号化等のプロテクトは，数学の論文に於ける定理や証明の暗号化の等しい物として厳しく禁止，拝斥される．また配布手数料は無料を原則とし，止むを得ない時でも実費のみしか請求してはならない．

- 収集や配布や情報伝達の媒体は出来るだけUNIX (tar format) のデータカートリッジかMS-DOS (PC-DOS), MAC-OSのディスク，あるいはE-mail (電子メイル) とする．その他の方法でも最終的にコンピュータが読めれば収集の対象とする．場合に因っては印刷物も収集するが，配布の対象とはしない．

2 経過と提案

準備状況 今迄に集まった物は以下の通りである. 特記しない場合はソースプログラムが存在している.

- R. P. Brent (Australian National University) による多倍長計算の為の汎用FORTRANプログラムパッケージ, Ver. 17/02/1977.
- 中村 憲 (東京都立大学 理学部) による大型計算機上の純三次体の基本単数及び類数の計算の為のFORTRANプログラム, Ver. 28/02/84.
- J. H. Silverman (Brown University) によるMAC-OS上の楕円曲線計算の為のZBASICプログラム (ソース無し), Ver. 17/05/87.
- 中原 徹 (佐賀大学 理工学部) による大型計算機上の実二次体の類群の3部分群の構造探査のFORTRANプログラム (印刷物), Ver. ??/??/87.
- 斉藤 美千代 (上智大学 理工学部) によるVAX/VMS上の二次体の類数と類群計算の為のFORTRANプログラム, Ver. ??/??/87.
- 中村 憲 (東京都立大学 理学部) によるUNIX上の Cyclo-Elliptic 法を用いた 2, 3, 4, 6 次体の計算のMACSYMAプログラム, Ver. 01/09/89.
- 鈴木 治郎 (信州大学 医療技術短期大学部) による大型計算機上の Fermat 予想の計算の為のFORTRANプログラム, Ver. 22/11/89.
- M. Pohst, J. G. von Schmettow (Universität Düsseldorf) 等による代数体の不変量を計算する数論専用の汎用FORTRANプログラム パッケージであるKANT, Ver. 11/04/90.

- 木田 祐司 (立教大学 理学部) によるMS-DOS上の数論専用の多倍長計算ツールであるUBASIC86 Ver. 8.12 (ソース無し) と, その応用プログラム, Ver. 05/09/90.
- 金子 昌信 (京都工芸繊維大学) による類多項式計算の為のMAC-OS上のMATHEMATICAプログラム, Ver. 18/02/91.
- 山村 健 (防衛大学校) によるMS-DOS上の 2 次体の計算と多項式の計算の C プログラム, Ver. 24/09/90 (及びソース無しの Ver. 27/02/91).
- 真島 陽一 (上越教育大学) による非正則素数計算のMS-DOS上の (一部機械語を含む)PASCALプログラム, Ver. 23/04/91.

配布の計画 データやプログラムの配布は以下の計画で実施する.

データ 少量の計算結果の数表は通常の可読コードの形式で全般的に配布する. 大量のデータは希望があった場合にのみ配布する事とする. むしろ計算の為のプログラムの配布を中心とする.

プログラム 先ず, 収集したプログラムを整理して原型のままで配布する. 次に, 汎用であるKANTをUNIXに実現して, それを中心として収集したプログラムの主な部分を組み込んだ整数論のツールを完成して配布する. 今後 Saarbrücken の数論専用の数式処理システムであるSIMATH, 又 Bordeaux を中心とした楕円曲線の有理点の計算を含むPARIS等の数論専用のソフトウェアを取得する. 更に,UBASICも併せて少なくともUNIXの上で走る整数論のパッケージを完成する.

希望

- 情報の迅速な交流の為に連絡のセンターを複数置きたい. ハードウェ

アの便に恵まれていて, しかも E-mail の使える方が良い. 現在迄に確定しているのは別記の通りである.

- データベースとソフトウェアの整備の為の協力者を募りたい. (若くて) エネルギーの有る人で, ソフトウェアの関心が強いか経験が豊かな人が良い.

連絡先

森田 康夫　東北大学 理学部 数学教室
〒980 仙台市 青葉区 荒巻 字青葉
E-mail ysmorita@jpntohok.bitnet

中村 憲　東京都立大学 理学部 数学教室
〒192-03 八王子市 南大沢 1-1
E-mail nakamula@tansei.cc.u-tokyo.ac.jp

中野 伸　名古屋大学 教養部 数学教室
〒464-01 名古屋市 千種区 不老町
E-mail e43263a@nucc.cc.nagoya-u.ac.jp

山本 芳彦　大阪大学 理学部 数学教室
〒560 豊中市 待兼山町 1-1
E-mail

宮脇 伊佐夫　九州大学 教養部 数学教室
〒810 福岡市 中央区 六本松 4-2-1
E-mail miyawaki@ec.kyushu-u.ac.jp